UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,979	08/31/2000	Adrian Shields	8490.00	3073

26889 7590 08/23/2005

MICHAEL CHAN
NCR CORPORATION
1700 SOUTH PATTERSON BLVD
DAYTON, OH 45479-0001

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/651,979	**Applicant(s)** SHIELDS, ADRIAN	
	Examiner Michael Pyzocha	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 21-38 are pending.

2. Response filed on 07/21/2005 has been received and considered.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 21-23, 33-34 and 38 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. The term "some" in claims 21, 33 and 38 is a relative term which renders the claim indefinite. The term "some" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. For the purpose of applying prior art the term "some" will be considered as "one or more".

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 21-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawan (US 20020062284) and further in view of Menezes et al (Handbook of Applied Cryptography).

As per claims 21 and 33, Kawan discloses a portable computer, with non-secure user-accessible memory communicating (sending and receiving) with an external terminal (see paragraphs 22 and 32).

Kawan fails to disclose a) storing records of events experienced by the computer in memory within the computer; b) using some of the records as seed for generating plain text of a first session key K1; and then c) encrypting K1, transmitting K1 (encrypted), and encrypting the communications.

However, Menezes et al teaches storing records of events and using the records as a seed for generating a key (see page

172) and this key being a session key (see page 494) and encrypting the session key (see page 552).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Menezes et al's key generation to generate a session key, which is encrypted, to be transmitted in the portable computer of Kawan.

Motivation to do so would have been to generate a true random bit sequence for a key (see page 171), to limit available cipher text for cryptanalytic attacks (see page 494) and to protect the session key (see page 552).

As per claims 22, 24, 26-30, and 38, the modified Kawan and Menezes et al system further includes repeating the above mentioned steps to create a new session key for each new transaction (see page 494) and receiving encrypted messaged encrypted by the session key (at both the portable computer and the external device) (see page 494 as applied to the communications of Kawan paragraph 32).

As per claims 23, 25, 31-32, and 34, the modified Kawan and Menezes et al system further includes the data used as the seed includes at least one element selected from the following group: recorded button selections, recorded pointer movements, recorded data entered by a user, current date setting, and current time setting (see page 172).

As per claims 35-37, the modified Kawan and Menezes et al system further includes the portable computer requires entry of a Personal Identification Number, PIN, prior to generation of the encryption key, and will not complete the transaction without the PIN (see paragraph 30).

Response to Arguments

1. Applicant's arguments filed 07/21/2005 have been fully considered but they are not persuasive. Applicant argues: the "some of the records" is not unclear; Kawan is not prior art; the modified Kawan and Menezes system fails to disclose the encrypted response; the modified system fails to disclose decrypting the response with K1; the combination is improper and lacks motivation; there is no expectation of success; Applicant requests elements be identified in the reference; Menezes teaches away from using "records" as a seed; if the second of two possibilities of Menezes occurs claim 21(a) would not be disclosed; only an assertion that claims 22-32, 34 and 38 is given which is improper; the PIN in Kawan cannot be used as a prerequisite for the encryption; and Kawan and Menezes are contradictory with respect to the session keys.

Regarding Applicant's argument that the "some of the records" is not unclear; the use of the word "some" in this phrase makes it unclear as to how many of the records are used if any at all. Also Applicant submitted claim 2 of US patent 5288949 as evidence that the office allows the use of the word "some" in a claim, however, this case has no relation to the present application.

Regarding Applicant's argument that Kawan is not prior art, from 901.02 of the MPEP: "a patent application publication published under 35 U.S.C. 122(b) is available as prior art under 35 U.S.C. 102(e) as of the earliest effective U.S. filing date of the published application" and Kawan has an application date of January 30, 1998 which is over six months earlier than Applicant's claimed foreign priority of September 1, 1999.

Regarding Applicant's argument that the modified Kawan and Menezes system fails to disclose the encrypted response, the combined references teach that all data exchanged between the portable computer and external computer is encrypted therefore the information and data interchange between the PDA and ATM of Kawan is encrypted. By definition (taken from answers.com) interchange means to exchange which means, "To give in return for something received." This clearly defines a response, so the modified Kawan and Menezes system discloses an encrypted response.

Regarding Applicant's argument that the modified system fails to disclose decrypting the response with K1, since K1 is a session key and in Menezes the session keys are secret keys (p 494 #4) the same key is used for encryption and decryption. Therefore the encrypted response (as discussed above) would be encrypted with the session key K1 and decrypted using K1.

Regarding Applicant's argument that the combination is improper because of the modification of Kawan, the modifications would not change the principle operation of the prior art invention because Kawan already performs encryption using a key and the modification only adds a key generation method and a more extensive encryption method, neither of which would change the principle operation of the Kawan system.

Regarding Applicant's argument that there is no expectation of success in the combination, based on the above and below responses it is clear how a successful combination is expected.

Regarding Applicant's argument that the combination lacks motivation, Applicant argues five problems. With respect to the first problem, the methods described on pages 171-172 are ways to produce true random bits. With respect to the second problem, Menezes teaches that software can be used to produce the true random bits and since portable computers can run software it would not be as great an achievement as Applicant suggests. Regarding the third problem, Applicant suggests that only one source would be needed; however, Kawan is needed to for the system in which the sequences are produced. With respect to the fourth problem, the limiting of the available cipher text is when using a session key as opposed to using the same key every different time the two parties communicate. With respect to the fifth problem, the encryption of the session key provides confidentiality of the session key, which provides motivation to use a session key with the above combination to produce the limitations of claim 21.

Regarding Applicant's request that elements be identified in the references, the "seed" is disclosed on page 172 of Menezes where the sample processes are sampled and fed into a hashing function to produce the random sequence, which makes the sample processes the "seed". "key K1", is the session key as described above. The "encrypted response" the "encrypted response" received by a "portable computer," and decrypting the "encrypted response" using K1 have been fully addressed above.

Regarding Applicant's argument that Menezes teaches away from using "records" as a seed, Applicant first argues that because Menezes states that the generator must not be subject to observation, the user-accessible memory of Kawan cannot be used, however in part (ii) Menezes teaches many operations to which the user has access to create the random sequence and therefore does not teach away from the combination.

Applicant further argues that if the second of two possibilities of Menezes occurs claim 21(a) would not be disclosed, however, Menezes teaches that the sources should be put through a hashing function and when doing this, the events must be stored.

The "records" are the information stored in the memory (which is the "user-accessible memory") described in Kawan paragraphs 22 and 32. The "seed" has been described above.

Regarding Applicant's argument that only an assertion that claims 22-32, 34 and 38 is given which is improper, however the rejection of these claims have a citation of where the limitation can be found.

Regarding Applicant's argument that the PIN in Kawan cannot be used as a prerequisite for the encryption, Kawan requires a verified PIN before any communication can begin and therefore before any encryption can occur.

Regarding Applicant's argument that Kawan and Menezes are contradictory with respect to the session keys, Kawan teaches the encrypted information being used for one or multiple transactions and because he teaches it for a single transaction the references do not contradict.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

E. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER